NOKIA

The security architecture of 5G networks and how it could evolve towards 6G

Dr. Stefan Wevering
stefan.wevering@nokia.com

Monday, 04-10-2021

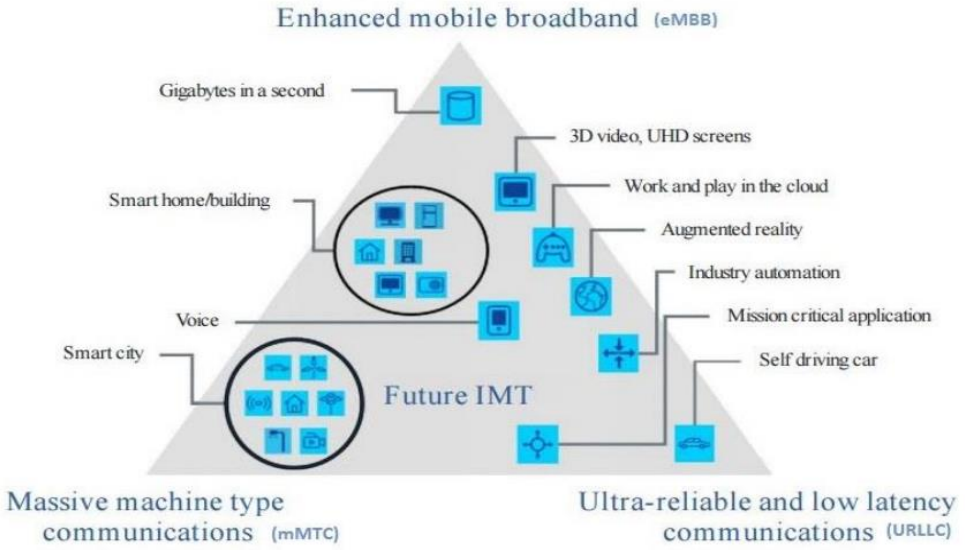
Agenda

- The “magic” triangle of 5G technologies
- Overview of 5G attack vectors
- Security improvements in 3GPP 5G standardization
- After 5G is before 6G
- Conclusions

The “magic” triangle of 5G technology

Three corners of the “magic” triangle of 5G

- Enhanced mobile broadband (eMBB) – Peak data rates of up to 10 Gbit/s
- Massive machine-type communications (mMTC) – thousands of connected sensors and actors
- Ultra-reliable and low latency communications (URLLC) – end-to-end latencies down to 5 ms and reliabilities up to 99,9999%



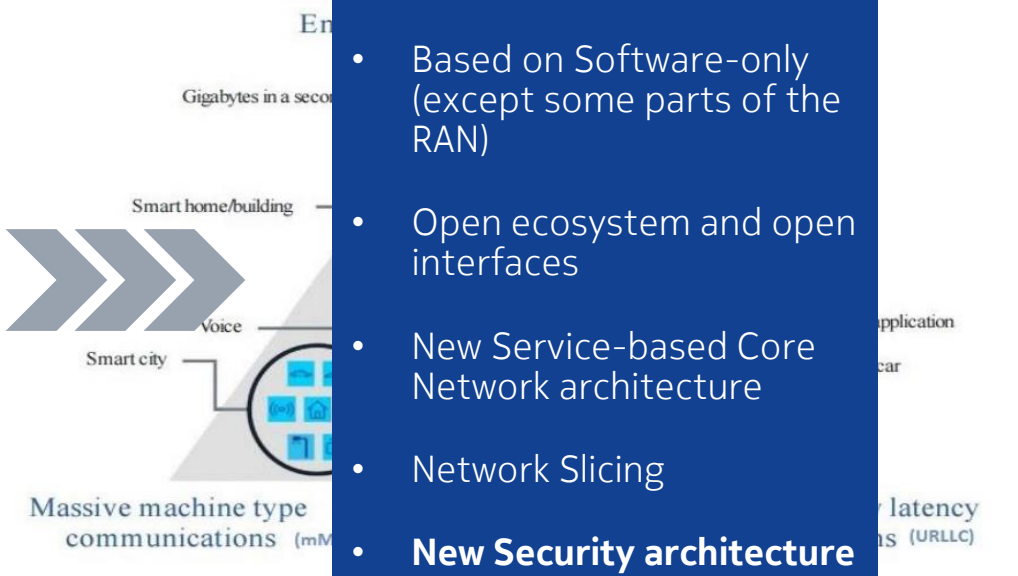
IMT: International Mobile Telecommunications

Source: 5G Whitepaper 2, NGMN Alliance, July 2020

The “magic” triangle of 5G technology

Three corners of the “magic” triangle of 5G

- Enhanced mobile broadband (eMBB) – Peak data rates of up to 10 Gbit/s
- Massive machine-type communications (mMTC) – thousands of connected sensors and actors
- Ultra-reliable and low latency communications (URLLC) – end-to-end latencies down to 5 ms and reliabilities up to 99,9999%

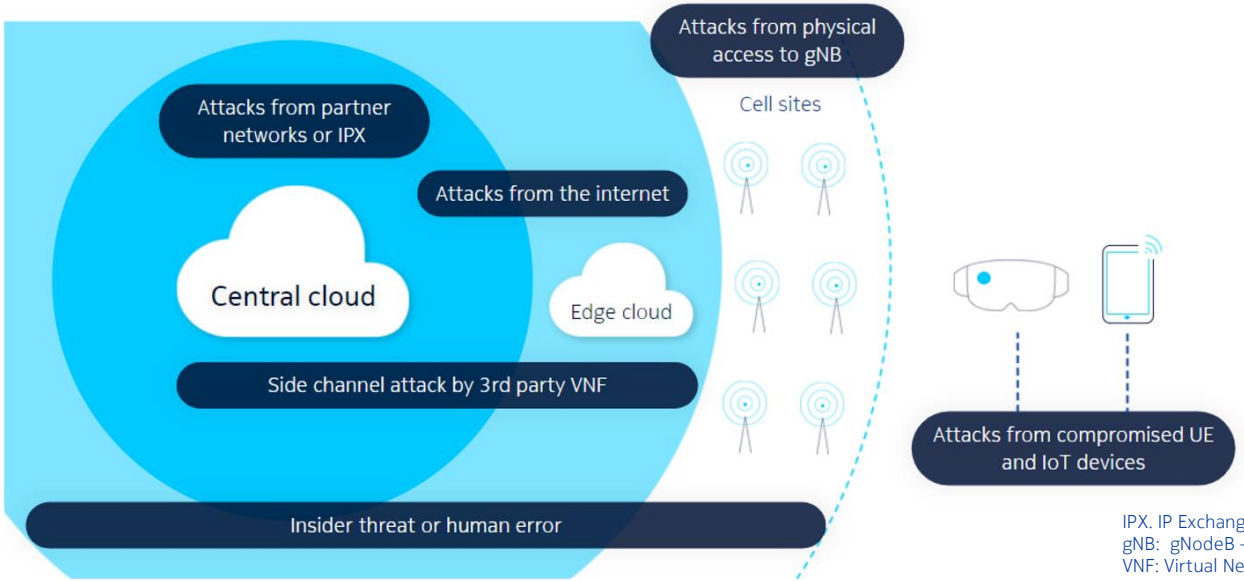


IMT: International Mobile Telecc

Requires a completely new network architecture

- Based on Software-only (except some parts of the RAN)
- Open ecosystem and open interfaces
- New Service-based Core Network architecture
- Network Slicing
- **New Security architecture**

Overview of the 5G attack vector

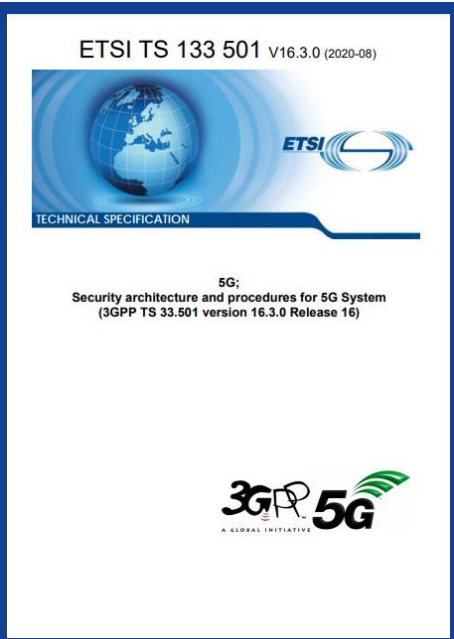


IPX. IP Exchange – interconnection of different operator's IP networks
gNB: gNodeB – Base Station of the 5G network
VNF: Virtual Network Function

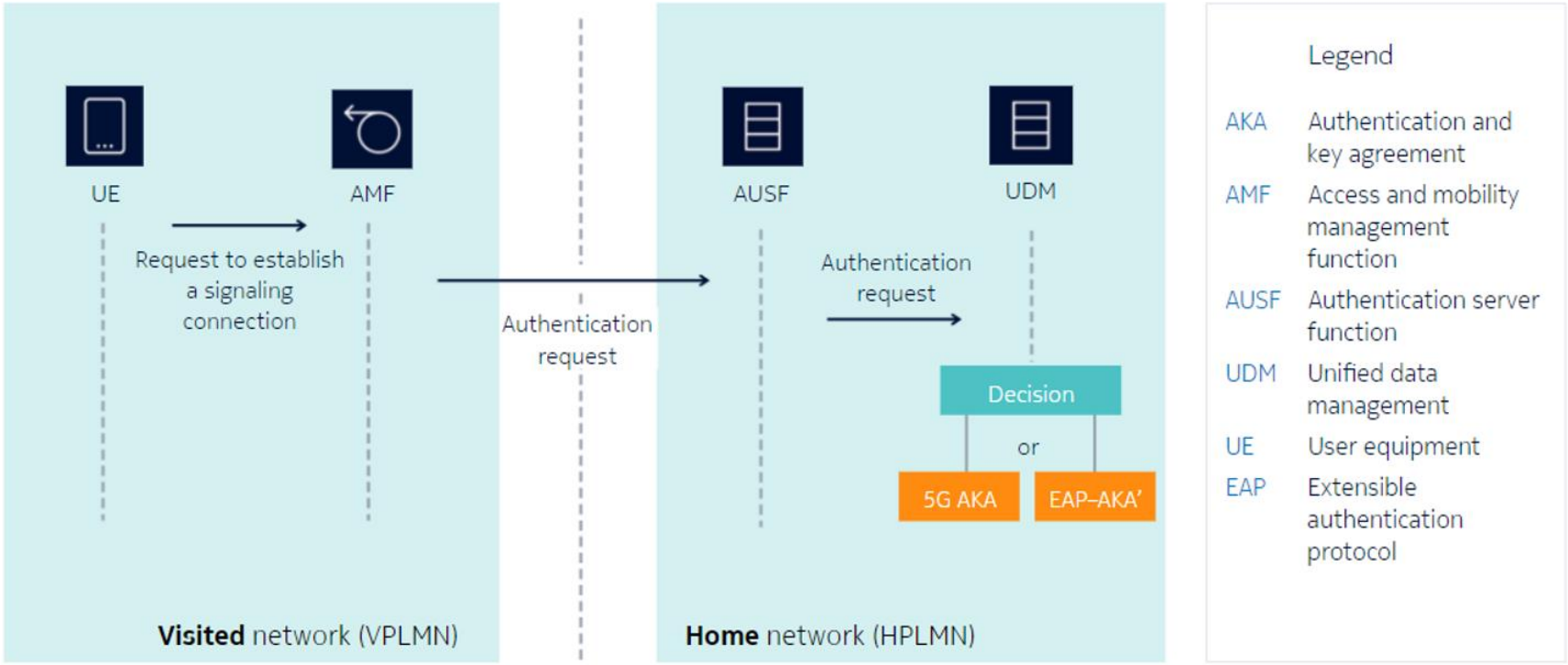
The edge-based perimeter for 5G security:
Always apply protection mechanisms at the edge of the network, where attackers may want to enter it!

3GPP 5G Standardization Overview:
Six security improvements in 5G

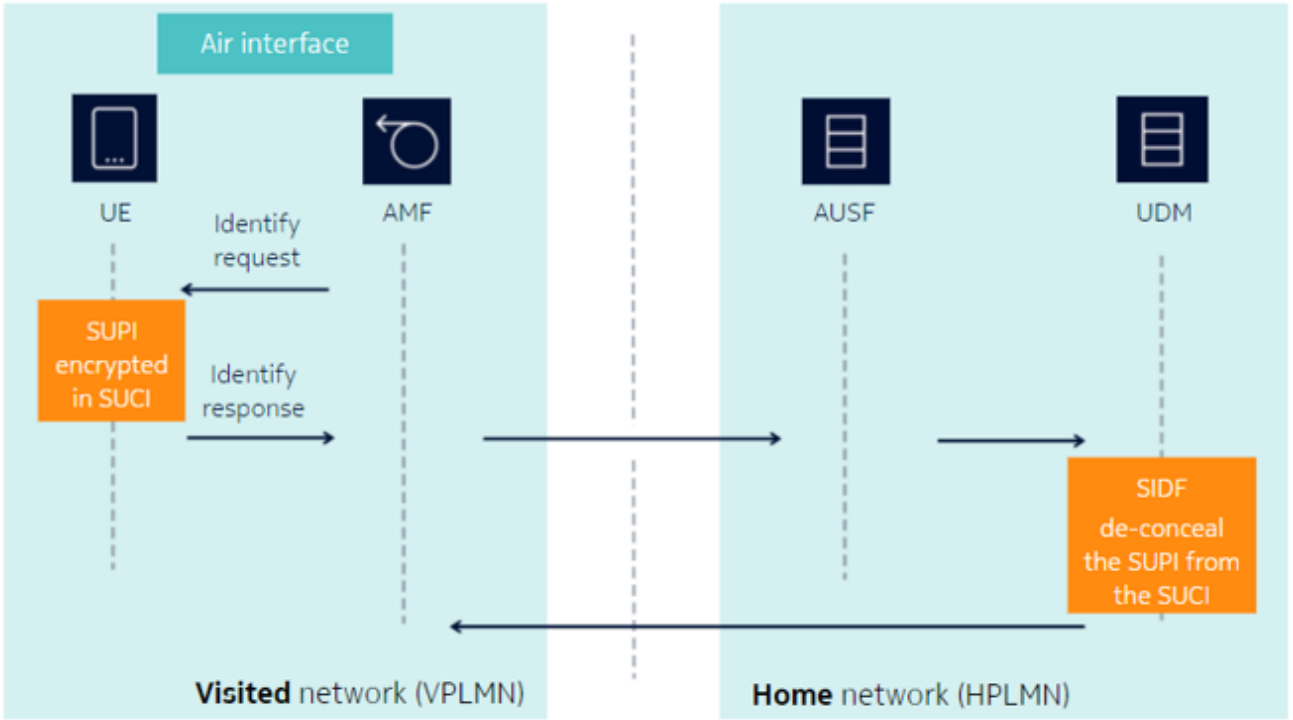
1. **New access-agnostic authentication framework**
2. **Enhanced subscription privacy**
3. **User plane integrity protection**
4. **EAP-based “secondary” authentication**
5. **Security for Service-based interfaces**
6. **Enhancement for interconnection security**



1 New access-agnostic authentication framework



2 Enhanced Subscription Privacy

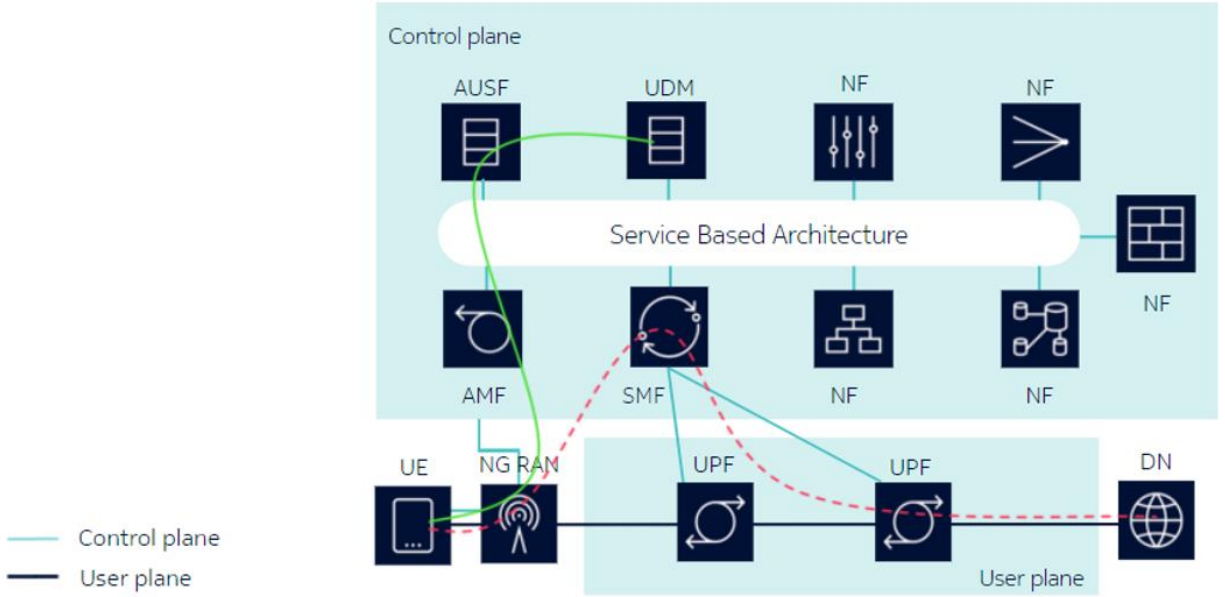


Legend

AMF	Access and Mobility Management Function
AUSF	Authentication Server Function
SIDF	Subscription Identifier De-concealing Function
SUCI	Subscription Concealed Identity
UDM	Unified Data Management
UE	User Equipment

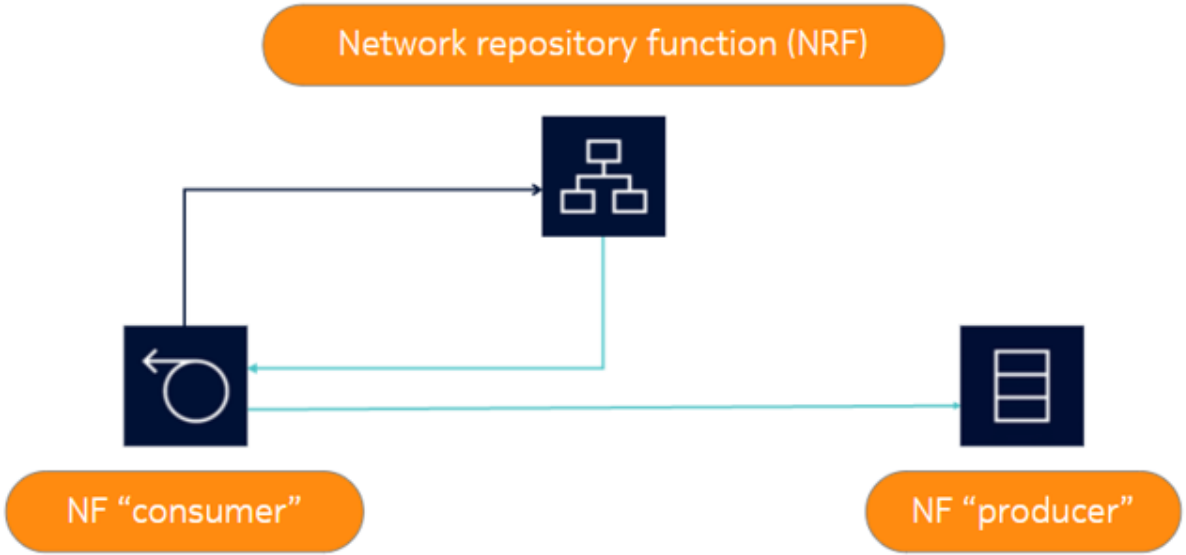
3 User plane integrity on the radio interface

4 EAP-based “secondary authentication” for UE



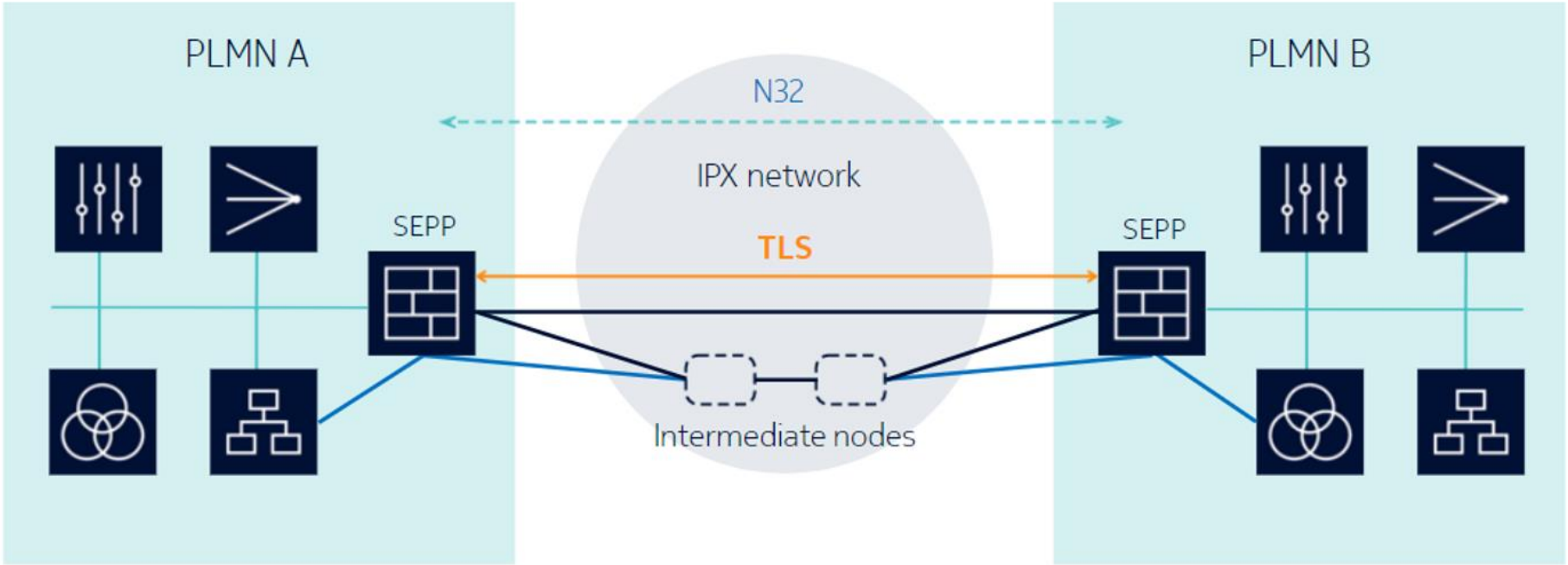
Flexible and secure authentication between a UE and an external data network

5 Security for Service-based interfaces



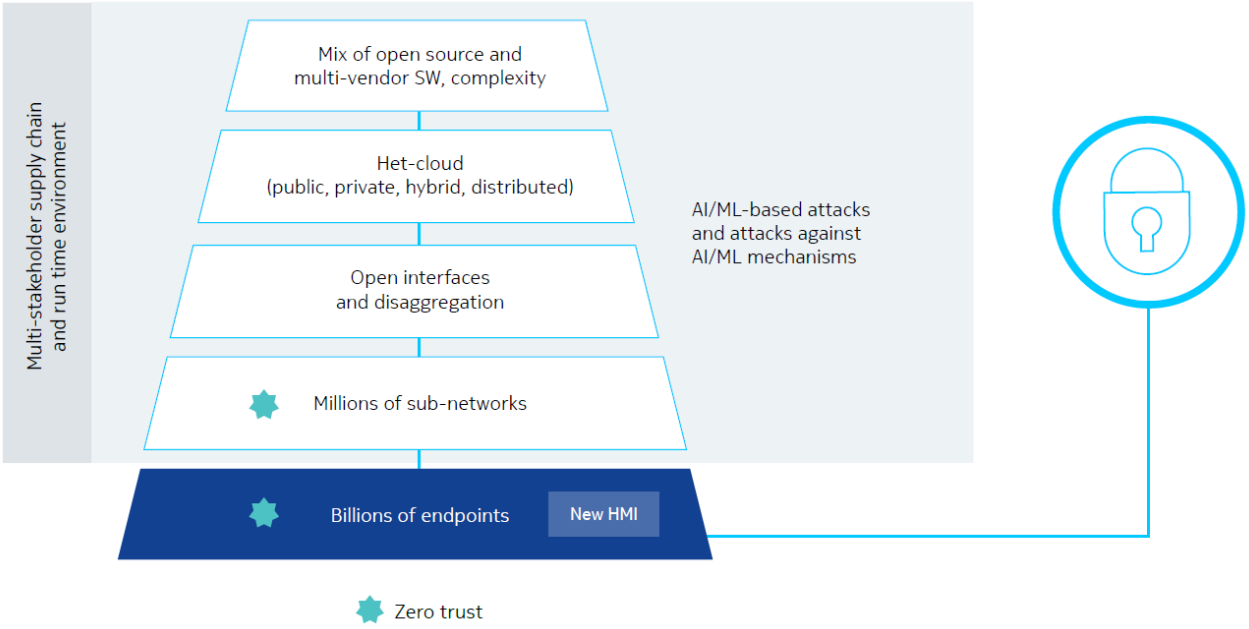
Token-based authorization of service requests to network functions, using the OAuth 2.0 framework

6 Interconnection security in 5G Networks



After 5G is before 6G

Potential dimensions of the 6G threat vector



Source: V. Ziegler et al., "Security and trust in the 6G era", Nokia Bell Labs Wihtepaper, 2021

The network needs to be protected against attacks coming

- from billions of connected endpoints, and
- from millions of attached subnetworks

Both cannot be considered trustworthy

Additionally,

- open interfaces and disaggregation
- deploying Het-Clouds, and
- the complexity due to mixing of open source and mv SW

lead to additional security threats

After 5G is before 6G

As the capabilities of 6G will rise compared to 5G, so will the technological complexity.

Regarding cyber security and cyber resilience, there are multiple concepts that may be of high importance, such as:

- Automated SW creation that eliminates in-built vulnerabilities by means of AI/ML
- Automated closed-loop security operations across applications, services, data storage and access, and Network Function execution environments
- New privacy preserving technologies, e.g., multi-party computation, homomorphic encryption, and edge validation for data integrity and privacy assurance
- Quantum safe security, based on quantum computing
- Enhanced physical layer security
- Distributed ledger technologies, e.g., blockchain, for specific 6G use cases, like trusted roaming and autonomous device management

5G is not the end of the story – the next challenge is 6G, potentially being realized in the 2030s

Conclusions

Security in 5G networks is a complex topic that needs to be considered in an end-to-end context.

The transition from HW- to SW-based communications in 5G Networks opens the door for new security attacks.

The threat potential is increasing when moving from 5G to 6G – we need a set of security technology enablers for 6G, enhanced by AI/ML and cyber-resilience.

As time goes by, attackers will find new ways to threaten 5G and 6G networks, so that regular adaptations to the security architecture become a necessity.